

UNITED STATES DISTRICT COURT

for the
Western District of Washington

FILED	LODGED
RECEIVED	
OCT 10 2019	
CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)Three subject digital devices, more fully described in
Attachment A

Case No. MJ19-5206

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Three subject digital devices, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

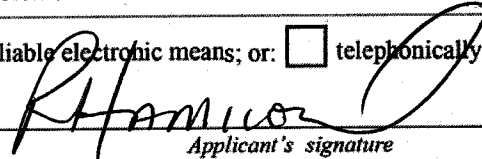
Code Section	Offense Description
21 U.S.C. § 841, 846	Drug distribution & conspiracy
18 U.S.C. § 1956	Money laundering

The application is based on these facts:

- ☒ See Affidavit of TFO Ryan Hamilton, continued on the attached sheet.

- ☒ Delayed notice of 90 days (give exact ending date if more than 30 days: 01/07/2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

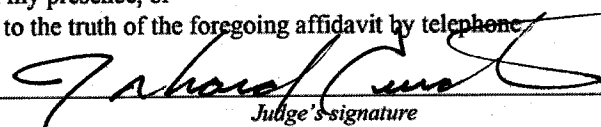
Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.


Applicant's signature

Ryan Hamilton, DEA Task Force Officer
Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/10/19


Judge's signature

City and state: Tacoma, Washington

J. Richard Creatura, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Ryan J. Hamilton, Task Force Officer, Drug Enforcement Administration (DEA), United States Department of Justice, being first duly sworn on oath, depose and state:

MY BACKGROUND AND QUALIFICATIONS

1. I am a duly commissioned Police Investigator for the Lakewood Police Department and a Task Force Officer (TFO) with the Drug Enforcement Administration (DEA). Accordingly, I am an investigative or law enforcement officer within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. I have been employed by the Lakewood Police Department since October 2004, most recently in the Narcotics unit. From 2001 to October 2004, I was a sworn deputy of the Pierce County Sheriff's Department working on contract with the City of Lakewood. My formal training includes an Associate's Degree in Applied Science in Law Enforcement from Green River Community College and two additional years at the University of Washington working towards a Bachelor's Degree in Law, Society, and Justice (I left one quarter prior to graduation when I was hired by the Pierce County Sheriff's Department). My coursework included classes in Criminal Procedure and Criminal Law.

2. Upon joining the Pierce County Sheriff's Department, I completed 720 hours of training at the Basic Law Enforcement Academy at the Washington State Criminal Justice Training Center (CJTC), where I was trained in the areas of Criminal Investigations, Narcotics Investigations, Interview Skills, Criminal Law, Criminal Procedures, Court Orders, and Search Warrants. I have also completed the 80-hour CJTC Undercover Operations/Investigations School and an 80-hour CJTC Basic Narcotics

1 Investigator course. I served as a Firearms Instructor from 2004 to 2019 and I am
2 currently a Field Training Officer (FTO) with the focus of training and evaluating newly
3 hired police officers.

4 3. I am familiar with investigations of drug trafficking organizations, methods
5 of importation and distribution of controlled substances, and financial investigations. I
6 have participated in numerous investigations involving organizations trafficking in
7 controlled substances which have resulted in arrests of drug traffickers, seizures of
8 controlled substances, and assets. My training and experience have involved, among
9 other things: (1) the debriefing of defendants, witnesses, and informants, as well as others
10 who have knowledge of the distribution and transportation of controlled substances and
11 of the laundering and concealment of proceeds of drug trafficking; (2) surveillance; (3)
12 analysis of documentary and physical evidence; and (4) the "undercover" purchases of
13 controlled substances and negotiations of illegal money laundering transactions

14 4. I have planned, participated in, and supervised the execution of more than
15 100 search warrants authorizing the search of locations associated with narcotic
16 traffickers and their co-conspirators, such as residences, businesses, storage facilities,
17 outbuildings, safety deposit boxes, and vehicles. I have testified in grand jury
18 proceedings and written reports in the course of investigations. I have monitored or
19 overheard numerous calls or meetings between informants or undercover agents, and
20 drug traffickers. These investigations have resulted in state and federal prosecutions of
21 individuals who have possessed, imported, or distributed controlled substances, including
22 marijuana, cocaine, methamphetamine, heroin, and prescription medications, as well as
23 the seizure of those illegal drugs and the proceeds from their sales. As a result of these
24 investigations, I have become familiar with methods and techniques used by narcotics
25 traffickers to import narcotics into the United States and distribute those narcotics within
26 the United States.

27 5. I have participated in investigations which involved drug traffickers using
28 telephone communication as a means of communicating with their associates,

1 confidential informants, cooperating individuals and undercover officers. I have also
2 worked and consulted with numerous law enforcement officers experienced in narcotics
3 investigations. As a result, I am familiar with how drug traffickers speak to each other
4 and generally conduct business. For example, I am aware that drug traffickers discussing
5 criminal matters over the phone often speak in code or in vague terms. I am also aware
6 that these subjects frequently (1) provide false subscriber information to the service
7 providers, (2) use phones which are subscribed to under identities other than their own,
8 and (3) change phones in order to avoid detection by law enforcement. This training and
9 experience forms the basis for my opinions expressed below. All dates and times listed
10 below are approximate unless otherwise noted.

11 **PURPOSE OF AFFIDAVIT**

12 6. This Affidavit is submitted in support of an application for a warrant to
13 search three cellular phones (collectively, the "subject digital devices") seized on October
14 7, 2019, and presently in the secure custody of the DEA in Tacoma, Washington, for
15 evidence, fruits and instrumentalities of drug trafficking and money laundering crimes
16 committed by Doriam German MORENO-Rocha and Adrian Alberto SANCHEZ-
17 Esparza, in violation of Title 21, United States Code, Sections 841(a)(1) and 846, and
18 Title 18, United States Code, Section 1956, as further described in Attachment B.

19 7. The subject digital devices are described as follows:

- 20 a. A Red Apple iPhone in a clear protective case (marked as DEA
21 Non-Drug Exhibit N-8);
22 b. A Black Samsung phone in a gray and black case (marked as DEA
23 Non-Drug Exhibit N-7; and
24 c. An Apple iPhone in a red case (marked as DEA Non-Drug Exhibit
25 N-9).

26 8. The three subject digital devices were seized during a traffic stop and
27 subsequent arrest of Doriam German MORENO-Rocha (aka "Popeye") and Adrian
28 Alberto SANCHEZ-Esparza, which occurred on October 7, 2019, in Kent, Washington.

1 9. I make this request based on the evidence described below, which
 2 establishes probable cause to believe that the subject digital devices were used to
 3 facilitate drug trafficking and money laundering crimes in the Western District of
 4 Washington and elsewhere in violation of 21 U.S.C. §§ 841 and 846, and 18 U.S.C. 1956,
 5 and that the information collected pursuant to the warrant will further the investigation of
 6 these violations.

7 10. Specifically, the warrant would authorize the forensic examination of the
 8 subject digital devices for the purpose of identifying and seizing the electronically stored
 9 data more particularly described in Attachment B.

10 **SOURCES OF INFORMATION**

11 11. I have obtained the facts set forth in this Affidavit through my personal
 12 participation in the investigation described below; from oral and written reports of other
 13 law enforcement officers; from witnesses and informants cooperating with law
 14 enforcement, and from records, documents and other evidence obtained during this
 15 investigation. I have obtained and read official reports prepared by law enforcement
 16 officers participating in this investigation and in other investigations.

17 12. Since I am submitting this Affidavit for the limited purpose of establishing
 18 probable cause to obtain search warrants for the cell phones identified above, I have set
 19 forth only the facts that I believe are necessary to establish probable cause for these
 20 warrants. As set forth herein, I believe Doriam German MORENO-Rocha and Adrian
 21 Alberto SANCHEZ-Esparza used these phones to facilitate drug trafficking and money
 22 laundering crimes.

23 **TECHNICAL TERMS**

24 13. Based on my training and experience, and consultation with other
 25 investigators, I use the following technical terms to convey the following meanings:

26 a. Wireless telephone: A wireless telephone (or mobile telephone, or
 27 cellular telephone) is a handheld wireless device used for voice and data communication
 28 through radio signals. These telephones send signals through networks of
 transmitter/receivers, enabling communication with other wireless telephones or

1 traditional "land line" telephones. A wireless telephone usually contains a "call log,"
 2 which records the telephone number, date, and time of calls made to and from the phone.
 3 In addition to enabling voice communications, wireless telephones offer a broad range of
 4 capabilities. These capabilities include: storing names and phone numbers in electronic
 5 "address books;" sending, receiving, and storing text messages and e-mail; taking,
 6 sending, receiving, and storing still photographs and moving video; storing and playing
 7 back audio files; storing dates, appointments, and other information on personal
 8 calendars; and accessing and downloading information from the Internet. Wireless
 9 telephones may also include global positioning system ("GPS") technology for
 10 determining the location of the device.

11 b. Tablet: A tablet is a mobile computer, typically larger than a phone
 12 yet smaller than a notebook that is primarily operated by touching the screen. Tablets
 13 function as wireless communication devices and can be used to access the Internet
 14 through cellular networks, "Wi-Fi" networks, or otherwise. Tablets typically contain
 15 programs called "apps," which, like programs on a personal computer, perform different
 16 functions and save data associated with those functions. Apps can, for example, permit
 17 accessing the Web, sending and receiving e-mail, accessing banking sites, and
 18 participating in Internet social networks. A common example of a tablet is an Apple
 19 iPad.

20 c. Internet: The Internet is a global network of computers and other
 21 electronic devices that communicate with each other. Due to the structure of the Internet,
 22 connections between devices on the Internet often cross state and international borders,
 23 even when the devices communicating with each other are in the same state.

24 **COMPUTERS, WIRELESS TELEPHONES/TABLETS, ELECTRONIC** 25 **STORAGE, AND FORENSIC ANALYSIS**

26 14. Based on my knowledge, training, and experience, I know that digital
 27 devices (including wireless telephones, tablets, and personal computers including
 28 laptops) and electronic storage media can store information for long periods of time.
 Similarly, things that have been viewed via the Internet are typically stored for some
 period of time on the device used to access the Internet. This information can sometimes
 be recovered with forensic tools.

15. There is probable cause to believe that things that were once stored on the
 subject digital devices may still be stored there, for at least the following reasons:

1 a. Based on my knowledge, training, and experience, I know that
2 computer files or remnants of such files can be recovered months or even years after they
3 have been downloaded onto a storage medium, deleted, or viewed via the Internet.
4 Electronic files downloaded to a storage medium can be stored for years at little or no
5 cost. Even when files have been deleted, they can be recovered months or years later
6 using forensic tools. This is so because when a person “deletes” a file on a computer, the
7 data contained in the file does not actually disappear; rather, that data remains on the
8 storage medium until it is overwritten by new data.

9 b. Therefore, deleted files, or remnants of deleted files, may reside in
10 free space or slack space—that is, in space on the storage medium that is not currently
11 being used by an active file—for long periods of time before they are overwritten. In
12 addition, a computer’s operating system may also keep a record of deleted data in a
13 “swap” or “recovery” file.

14 c. Wholly apart from user-generated files, computer storage media—in
15 particular, computers’ internal hard drives—contain electronic evidence of how a
16 computer has been used, what it has been used for, and who has used it. To give a few
17 examples, this forensic evidence can take the form of operating system configurations,
18 artifacts from operating system or application operation, file system data structures, and
19 virtual memory “swap” or paging files. Computer users typically do not erase or delete
20 this evidence, because special software is typically required for that task. However, it is
21 technically possible to delete this information.

22 d. Similarly, files that have been viewed via the Internet are sometimes
23 automatically downloaded into a temporary Internet directory or “cache.”

24 16. As further described in Attachment B, this application seeks permission to
25 locate not only electronically stored information that might serve as direct evidence of the
26 crimes described on the warrants, but also forensic evidence that establishes how the
27 subject digital devices were used, the purpose of their use, who used them, and when.
28 There is probable cause to believe that this forensic electronic evidence might be on the
subject digital devices because:

 a. Data on the storage medium can provide evidence of a file that was
once on the storage medium but has since been deleted or edited, or of a deleted portion
of a file (such as a paragraph that has been deleted from a word processing file). Virtual
memory paging systems can leave traces of information on the storage medium that show
what tasks and processes were recently active. Web browsers, e-mail programs, and chat
programs store configuration information on the storage medium that can reveal

1 information such as online nicknames and passwords. Operating systems can record
2 additional information, such as the attachment of peripherals, the attachment of USB
3 flash storage devices or other external storage media, and the times the computer was in
4 use. Computer file systems can record information about the dates files were created and
the sequence in which they were created.

5 b. As explained herein, information stored within a computer and other
6 electronic storage media may provide crucial evidence of the “who, what, why, when,
7 where, and how” of the criminal conduct under investigation, thus enabling the United
8 States to establish and prove each element or alternatively, to exclude the innocent from
9 further suspicion. In my training and experience, information stored within a computer
10 or storage media (e.g., registry information, communications, images and movies,
11 transactional information, records of session times and durations, internet history, and
12 anti-virus, spyware, and malware detection programs) can indicate who has used or
13 controlled the computer or storage media. This “user attribution” evidence is analogous
14 to the search for “indicia of occupancy” while executing a search warrant at a residence.
15 The existence or absence of anti-virus, spyware, and malware detection programs may
16 indicate whether the computer was remotely accessed, thus inculcating or exculpating the
17 computer owner and/or others with direct physical access to the computer. Further,
18 computer and storage media activity can indicate how and when the computer or storage
19 media was accessed or used. For example, as described herein, computers typically
20 contain information that log: computer user account session times and durations,
21 computer activity associated with user accounts, electronic storage media that connected
22 with the computer, and the IP addresses through which the computer accessed networks
23 and the internet. Such information allows investigators to understand the chronological
24 context of computer or electronic storage media access, use, and events relating to the
crime under investigation.¹ Additionally, some information stored within a computer or
electronic storage media may provide crucial evidence relating to the physical location of
other evidence and the suspect. For example, images stored on a computer may both
show a particular location and have geolocation information incorporated into its file
data. Such file data typically also contains information indicating when the file or image
was created. The existence of such image files, along with external device connection
logs, may also indicate the presence of additional electronic storage media (e.g., a digital
camera or cellular phone with an incorporated camera). The geographic and timeline
information described herein may either inculcate or exculpate the computer user. Last,

25
26 ¹ For example, if the examination of a computer shows that: a) at 11:00am, someone using the
27 computer used an internet browser to log into a bank account in the name of John Doe; b) at
28 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the
internet browser was used to log into a social media account in the name of John Doe, an
investigator may reasonably draw an inference that John Doe downloaded child pornography.

1 information stored within a computer may provide relevant insight into the computer
2 user's state of mind as it relates to the offense under investigation. For example,
3 information within the computer may indicate the owner's motive and intent to commit a
4 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt
(e.g., running a "wiping" program to destroy evidence on the computer or password
protecting/encrypting such evidence in an effort to conceal it from law enforcement).

5
6 c. A person with appropriate familiarity with how an electronic device
7 works may, after examining this forensic evidence in its proper context, be able to draw
8 conclusions about how electronic devices were used, the purpose of their use, who used
them, and when.

9 d. The process of identifying the exact electronically stored
10 information on a storage medium that are necessary to draw an accurate conclusion is a
11 dynamic process. Electronic evidence is not always data that can be merely reviewed by
12 a review team and passed along to investigators. Whether data stored on a computer is
13 evidence may depend on other information stored on the computer and the application of
knowledge about how a computer behaves. Therefore, contextual information necessary
to understand other evidence also falls within the scope of the warrant.

14 e. Further, in finding evidence of how a device was used, the purpose
15 of its use, who used it, and when, sometimes it is necessary to establish that a particular
16 thing is not present on a storage medium.

17 17. Because these warrants seek only permission to examine the subject digital
18 devices already in law enforcement's possession, execution of these warrants does not
19 involve the physical intrusion onto a premises. Consequently, I submit there is
20 reasonable cause for the Court to authorize execution of the warrants at any time in the
21 day or night.

22 SUMMARY OF PROBABLE CAUSE

23 18. Investigators with the Tacoma DEA and King County Sheriff's Office have
24 been conducting a joint investigation into the HERNANDEZ DTO since October of
25 2018. The HERNANDEZ DTO has been identified as a local drug distribution group
26 that obtains heroin and methamphetamine from Mexico-based sources and local sources.
27 The DTO then distributes these drugs in Western Washington. Investigators are currently
28 intercepting (with court authorization) phones used by DTO head Daniel HERNANDEZ,

1 DTO runner Norberto FLORES-Lopez, and local source of supply Omar SALAZAR.

2 This is the fourth period of authorized interception during the immediate investigation of
3 the HERNANDEZ DTO.

4 19. During these interception periods, investigators identified one of the DTO's
5 Mexico-based sources of supply as Juan MORENO-Rocha; MORENO-Rocha uses the
6 moniker "Cachin." Based on numerous intercepted calls, investigators knew that Juan
7 MORENO-Rocha supplied both heroin and methamphetamine to the DTO. Investigators
8 also learned from these intercepted communications that Juan MORENO-Rocha worked
9 with his brother, who went by the moniker "Popeye." Investigators believed that
10 "Popeye" could be Dorian MORENO-Rocha.

11 20. On October 4, 2019, starting at 10:02 a.m., investigators intercepted
12 multiple text messages between Daniel HERNANDEZ (TT1) and Juan MORENO-Rocha
13 (52-667-572-0000) regarding a shipment of drugs that Juan MORENO-Rocha was
14 planning on shipping to HERNANDEZ. Investigators had determined that Mexican
15 telephone number 52-667-572-0000 was associated with Juan MORENO-Rocha because
16 HERNANDEZ referred to the user of this phone number as "Cachin," a known moniker
17 for Juan MORENO-Rocha. The text message exchange between HERNANDEZ (TT1)
18 and Juan MORENO-Rocha was in Spanish and has been transcribed by DEA-contracted
19 linguists as follows:

20 HERNANDEZ (Session 7301): 22 for the dark one, family.

21 HERNANDEZ (Session 7303): I'll give you the information about the
22 water in an hour.

23 Juan MORENO-Rocha (Session 7315): Okay, sounds good. Thanks.

24 HERNANDEZ (Session 7332): I wanted to see if they were ready with
25 one of water, but they haven't taken
26 anything out.
27
28

1 HERNANDEZ (Session 7334): Honestly dude, I'm trying my best, but
 2 nothing is coming out, and I'm heading
 3 downhill very badly.

4 Juan MORENO-Rocha (Session 7336): Dude, you had told me 30 of water and
 5 25 of night, last time I had called you.

6 HERNANDEZ (Session 7338): Yes, but these guys aren't ready, dude.

7 HERNANDEZ (Session 7340): They haven't taken anything out.

8 21. Investigators later intercepted a call (Session 7344) between HERNANDEZ
 9 and Juan MORENO-Rocha. During this conversation, Juan MORENO-Rocha spoke to
 10 HERNANDEZ about HERNANDEZ making a payment. Juan MORENO-Rocha
 11 indicated he had a shipment of drugs ready to go, but said the people in Mexico wanted to
 12 get a payment from HERNANDEZ first. Following this call, investigators then
 13 intercepted multiple calls between HERNANDEZ and DTO members FLORES-Lopez
 14 and Fernando BAUTISTA-Sanchez in which HERNANDEZ attempted to collect money
 15 for the upcoming shipment of drugs.

16 22. At 7:16 p.m., investigators intercepted a call (Session 7584) between
 17 HERNANDEZ and Juan MORENO-Rocha. During this call, Juan MORENO-Rocha told
 18 HERNANDEZ, "I have a little surprise for you. Just like last time." HERNANDEZ
 19 replied, "Oh, really? What? Is your brother here already or what?" Investigators had
 20 previously identified Juan MORENO-Rocha's brother as a person who used the moniker
 21 "Popeye" and had tentatively identified him as Dorian German MORENO-Rocha, based
 22 on investigators' searches of social media accounts and law enforcement databases.
 23 During prior intercepted calls, investigators learned that "Popeye" worked with Juan
 24 MORENO-Rocha to traffic drugs from Mexico to the United States. Juan MORENO-
 25 Rocha answered HERNANDEZ's question, stating, "Yes, the dude is around there, and I
 26 wanted to see if he would call you....well, he is going to call you there, to see if you can
 27 meet him there." HERNANDEZ and Juan MORENO-Rocha continued to talk about
 28 HERNANDEZ meeting up with "Popeye," apparently to talk about the current

1 arrangement between HERNANDEZ and both Juan MORENO-Rocha and "Popeye."
2 HERNANDEZ told Juan MORENO-Rocha he was glad that "Popeye" was here so that
3 he (HERNANDEZ) could "focus more on the street."

4 23. Through additional intercepted calls, investigators learned that
5 HERNANDEZ was going to meet "Popeye" at an IHOP restaurant (at 610 Rainier
6 Avenue South, Renton, Washington) in the evening of October 4, 2019. Investigators
7 also learned that FLORES-Lopez was going to pick HERNANDEZ and take
8 HERNANDEZ to the meet. Investigators set up surveillance on the IHOP parking lot
9 and observed HERNANDEZ and FLORES-Lopez arrive at 8:27 p.m., in FLORES-
10 Lopez's father's vehicle (bearing Washington license BNS7043).

11 24. At 8:26 p.m., investigators intercepted a call (Session 7609) between
12 telephone number 206-712-9375 and HERNANDEZ (TT1). From the context of the call,
13 agents believed "Popeye" was the male user of 206-712-9375. "Popeye" stated that he
14 was taking an exit off the highway and would be to HERNANDEZ soon. At 8:37 p.m.,
15 investigators observed a silver BMW (bearing Washington license AGW4609) pull up to
16 the front of IHOP and park. A Hispanic male exited the vehicle; HERNANDEZ met the
17 male at the door and they both entered the business. Investigators researched the
18 licensing information for the BMW and learned it was registered to Juan MORENO-
19 Rocha's wife, Daniela Medina-Rosas at her father's address of 708 South Kenyan Street,
20 Seattle, Washington.

21 25. Investigators entered the IHOP and located HERNANDEZ sitting with the
22 male who exited Medina-Rosas' BMW. Investigators positively identified the male as
23 Dorian German MORENO-Rocha by comparison to an immigration enforcement photo
24 of Dorian MORENO-Rocha. HERNANDEZ sat and talked with Dorian MORENO-
25 Rocha from approximately 8:37 p.m. to 10:24 p.m. before leaving. FLORES-Lopez
26 picked up HERNANDEZ in the same vehicle they had arrived in, and Dorian
27 MORENO-Rocha left in the same vehicle he had arrived in.
28

1 26. On October 5, 2019, investigators intercepted multiple text messages
2 between HERNANDEZ (TT1) and DTO member Fernando BAUTISTA-Sanchez. These
3 texts started initially talking about "Popeye" wanting to meet with BAUTISTA-Sanchez,
4 but BAUTISTA-Sanchez not wanting to. At 10:44 a.m., investigators intercepted a text
5 (Session 7669) from HERNANDEZ (TT1) to BAUTISTA-Sanchez that read, "Honestly
6 man, it's good he came, I told pariente to not send water and he sent like 15 k." From
7 other information learned during the course of this investigation, investigators know
8 "Pariente" to be a reference to Juan MORENO-Rocha and "15 k" to mean 15 kilograms.
9 "Water" is a common code word for methamphetamine.

10 27. On October 6, 2019, at 8:30 p.m., investigators intercepted a call (Session
11 8199) between Doriam MORENO-Rocha (206-712-9375) and HERNANDEZ (TT1).
12 Both parties greeted each other. Doriam MORENO-Rocha then said, "I was checking,
13 you told me sixteen, but it's fifteen." HERNANDEZ replied, "No, it's sixteen." Doriam
14 MORENO-Rocha said, "No, it's five, five, four, and one." HERNANDEZ replied,
15 "Really?" Investigators believe this meant that HERNANDEZ had made a \$15,000.00
16 cash payment to Doriam MORENO-Rocha but thought he had paid \$16,000.00.

17 28. Doriam MORENO-Rocha then appeared to ask HERNANDEZ if the other
18 payment was going to be correct. Doraim MORENO-Rocha said, "I just checked it. I
19 checked it, and then I said, 'I am going to call you right away.' The other ones, are you
20 sure are the three two? Because I told them over there that what it was." HERNANDEZ
21 replied, "Thirty-two, yes. There are four packs of, of five, and then, uh, twelve of, of
22 one." This suggested that HERNANDEZ had packaged \$32,000.00 cash into four
23 bundles of \$5,000.00 each (totaling \$20,000.00) and twelve bundles of \$1,000.00 each
24 (totaling \$12,000.00). This also suggested to investigators that HERNANDEZ was
25 sending a total of \$47,000.00 to Mexico, via Doriam MORENO-Rocha, knowing that a
26 shipment of drugs was on its way to him (HERNANDEZ) in Washington.

27 29. Doriam MORENO-Rocha and HERNANDEZ continued to talk about the
28 shipment of drugs that was on its way. HERNANDEZ told Doriam MORENO-Rocha

1 that he (HERNANDEZ) was going to bring over gloves, a vacuum sealer, and tape.
2 HERNANDEZ then said, "We are going to check one, we are going to open one right?
3 So, we can see it?" Dorian MORENO-Rocha replied, "That's what I was thinking,
4 because it seems that one of them is one-six. We can open it, and then we'll divide that
5 one among us. This way we don't have to alter it, and avoid shrink it." HERNANDEZ
6 then replied, "Yes, we need to open it and check it. Valedor [ISLAS-Estrada] has
7 aluminum over there." Investigators believe that Dorian MORENO-Rocha was
8 implying that one of the inbound packages weighed only 16 ounces, and that they could
9 open that one to test it. When HERNANDEZ stated that ISLAS-Estrada has aluminum,
10 that suggested to investigators that heroin was included in the shipment with
11 methamphetamine (since burning heroin on aluminum foil is a way in which the quality
12 of heroin can be tested).

13 30. HERNANDEZ and Dorian MORENO-Rocha then discussed the shipment
14 itself. Dorian MORENO-Rocha told HERNANDEZ that the shipment was going to
15 arrive around 2:00 a.m. to 3:00 a.m. that night/morning. Dorian MORENO-Rocha and
16 HERNANDEZ agreed to meet at ISLAS-Estrada's residence around 6:00 a.m. (on
17 October 7, 2019) to get the drugs out of the load vehicle.

18 31. On October, 7, 2019, at approximately 5:45 a.m., investigators set up
19 surveillance on ISLAS-Estrada's residence (20631 26th Avenue South, Seatac,
20 Washington). Investigators checked the footage from mounted surveillance video camera
21 that points northbound on 26th Avenue South towards ISLAS-Estrada's residence.
22 Investigators noticed that an SUV had arrived at ISLAS-Estrada's residence at 2:31 a.m.,
23 and that the SUV appeared to have been followed by ISLAS-Estrada's vehicle (a white
24 2006 Honda Civic bearing Washington license BGY5960). Investigators also observed
25 (via the surveillance camera) that Dorian MORENO-Rocha appeared to arrive at ISLAS-
26 Estrada's residence at 6:40 a.m. Investigators on physical surveillance were able to
27 confirm that the last two digits on the license plate of a vehicle that had pulled up outside
28 the residence were "09," which was consistent with the license plate on the BMW

1 (Washington AGW4609) Doriam MORENO-Rocha had previously driven to meet
2 HERNANDEZ. Investigators noticed a silver Volkswagen arrive around the same time
3 (around 6:40 a.m.). Investigators knew that HERNANDEZ had previously used a silver
4 Volkswagen (bearing Washington license AVP1571) in the past, and that BAUTISTA-
5 Sanchez had been using it recently.

6 32. Investigators observed several people walking in and around the area of the
7 garage/carport, which is to the south of the residence. This was consistent with the
8 contents of the prior intercepted call regarding having to get the drugs out of the load car.
9 At 7:38 a.m., investigators saw (via the mounted surveillance camera and physical
10 surveillance) HERNANDEZ walk away from the area of ISLAS-Estrada's garage and
11 toward the Volkswagen. It did not appear that HERNANDEZ was carrying anything in
12 his hands when he went to the car; an intercepted call suggested that he was going to go
13 pick up his nephew and drive him to school.

14 33. At 8:16 a.m., investigators (via the mounted surveillance camera and
15 physical surveillance) noticed that someone drove Doriam MORENO-Rocha's BMW
16 into ISLAS-Estrada's garage area where investigators suspect the load vehicle was
17 parked. To investigators, there appeared to be no reason to do so unless the men were
18 planning on putting something into the vehicle and wanted to do it in privacy. At 8:37
19 p.m., investigators observed the BMW back out of ISLAS-Estrada's garage area and
20 drive away. Investigators confirmed the license plate was Washington AGW4609, i.e.,
21 the same vehicle Doriam MORENO-Rocha was seen previously using.

22 34. At 8:48 a.m., investigators conducted a traffic stop of the BMW. Doriam
23 MORENO-Rocha was driving and Adrian Alberto SANCHEZ-Esparza was the
24 passenger. Both were identified through their respective Mexico-issued photo IDs.
25 Because Doriam MORENO-Rocha and Adrian Alberto SANCHEZ-Esparza were both
26 acting nervous, investigators placed them in handcuffs for officer safety. A drug-
27 detection K9 gave a positive indication on the passenger's door area of the car.
28

1 35. Dorian MORENO-Rocha was in possession of the red Apple iPhone
2 (Exhibit N-8). Adrian SANCHEZ-Esparza was in possession of the Apple iPhone
3 (Exhibit N-9. The third cell phone (the Samsung in a black/gray case, Exhibit N-7) was
4 in the center console of the vehicle.

5 36. Investigators determined Dorian MORENO-Rocha and Adrian
6 SANCHEZ-Esparza were both in the county illegally. Officers with U.S. Immigration
7 and Customs Enforcement (ICE) responded and took custody of Dorian MORENO-
8 Rocha and Adrian SANCHEZ-Esparza. Investigators noticed that both of Adrian
9 SANCHEZ-Esparza's hands were recently cut up and scraped; these injuries were
10 consistent with him reaching into a trap or void area of a vehicle used to secrete
11 narcotics. Investigators took photos of his hands.

12 37. Investigators then searched the BMW and located a large duffel type bag in
13 the trunk of the vehicle. Inside this bag, investigators located approximately 15
14 kilograms of suspected methamphetamine and 5.5 kilograms of suspected heroin in
15 addition to cash and other evidentiary items. The drugs and the evidentiary items were
16 transported back to the DEA Tacoma and placed in the secure evidence room.

17 38. At 12:12 p.m., investigators intercepted a call (Session 8228) between
18 HERNANDEZ (TT1) and ISLAS-Estrada pertaining to HERNANDEZ and Juan
19 MORENO-Rocha trying to locate Dorian MORENO-Rocha. HERNANDEZ asked
20 ISLAS-Estrada what time "Popeye" and "Zorro" left. Investigators had intercepted
21 several calls previously where "Zorro" was described as a courier for the MORENO-
22 Rocha brothers, so this call suggested that "Zorro" was Adrian SANCHEZ-Esparza.
23 ISLAS-Estrada replied to HERNANDEZ that both Dorian MORENO-Rocha and Adrian
24 SANCHEZ-Esparza had left in the BMW with the drugs that had just been shipped up to
25 Washington.

COMMON CHARACTERISTICS OF DRUG TRAFFICKERS
AND MONEY LAUNDERERS

39. Based upon my training, experience, and participation in this and other investigations involving narcotics trafficking and money laundering, my conversations with other experienced investigators and law enforcement investigators with whom I work, and interviews of individuals who have been involved in money laundering and the trafficking of methamphetamine, cocaine, fentanyl and other drugs, I have learned and know the following.

40. Drug traffickers use mobile electronic devices including cellular telephones, tablets and other wireless communication devices to conduct their illegal trafficking business and money laundering activities. As described below, such equipment often contains evidence of these illegal activities.

41. Traffickers of controlled substances commonly maintain addresses, vehicles, or telephone numbers that reflect names, addresses, vehicles, and/or telephone numbers of their suppliers, customers, and associates in the trafficking organization, and it is common to find drug traffickers keeping records of said associates in cellular telephones and other electronic devices. Traffickers often maintain cellular telephones for ready access to their clientele and to maintain their ongoing narcotics business. Traffickers frequently change their cellular telephone numbers to avoid detection by law enforcement, and it is common for traffickers to use more than one cellular telephone at any one time.

42. Drug traffickers and Money Launderers use cellular telephones as a tool or instrumentality in committing their criminal activity. They use them to maintain contact with their suppliers, distributors, and customers. They prefer cellular telephones because, first, they can be purchased without the location and personal information that landlines require. Second, they can be easily carried to permit the user maximum flexibility in meeting associates, avoiding police surveillance, and traveling to obtain or distribute drugs and money. Third, they can be passed between members of a drug and money

1 conspiracy to allow substitution when one member leaves the area temporarily. Since
2 cellular phone use became widespread, every drug dealer and money launderer I have
3 interacted with has used one or more cellular telephones for his or her drug and money
4 business. I also know that it is common for drug traffickers and money launderers to
5 retain in their possession phones that they previously used, but have discontinued actively
6 using, for their drug trafficking and money laundering business. Based on my training
7 and experience, the data maintained in a cellular telephone used by a drug dealers and
8 money launderers is evidence of a crime or crimes. This includes the following:

9 a. The assigned number to the cellular telephone (known as the mobile
10 directory number or MDN), and/or the identifying telephone serial number (Electronic
11 Serial Number (ESN), Mobile Identification Number (MIN), International Mobile
12 Subscriber Identity (IMSI) number, or International Mobile Equipment Identity (IMEI)
13 number) are important evidence because they reveal the service provider, allow agents to
14 obtain subscriber information, and uniquely identify the telephone. This information can
15 be used to obtain toll records, to identify contacts by this telephone with other cellular
16 telephones used by co-conspirators, to identify other telephones used by the same
17 subscriber or purchased as part of a package, and to confirm if the telephone was
18 contacted by a cooperating source.

19 b. The stored list of recent received calls and sent calls is important
20 evidence. It identifies telephones recently in contact with the telephone user. This is
21 valuable information in a drug investigation because it will identify telephones used by
22 other members of the organization, such as suppliers, distributors and customers, and it
23 confirms the date and time of contacts. If the user is under surveillance, it identifies what
24 number he called during or around the time of a surveilled drug transaction or meeting.
25 Even if a contact involves a telephone user not part of the conspiracy, the information is
26 helpful (and thus is evidence) because it leads to friends and associates of the user who
27 can identify the user, help locate the user, and provide information about the user.
28

1 Identifying a defendant's law-abiding friends is often just as useful as identifying his
2 drug-trafficking and money laundering associates.

3 c. Stored text messages are important evidence, similar to stored
4 numbers. Agents can identify both drug associates, and friends of the user who likely
5 have helpful information about the user, his location, and his activities.

6 d. Photographs and videos on a cellular telephone are evidence because
7 they help identify the user, either through his or her own picture, or through pictures of
8 friends, family, and associates that can identify the user. Pictures also identify associates
9 likely to be members of the MLDTO organization. Also, digital photos often have
10 embedded "geocode" information within them. Geocode information is typically the
11 longitude and latitude where the photo was taken. Showing where the photo was taken
12 can have evidentiary value. This location information is helpful because, for example, it
13 can show where coconspirators meet, where they travel, and where assets might be
14 located.

15 e. Stored address records are important evidence because they show the
16 user's close associates and family members, and they contain names and nicknames
17 connected to phone numbers that can be used to identify suspects.

18 f. It is common for drug traffickers and money launderers to use
19 encrypted means of communication, such as WhatsApp, Silent Circle, Signal, Wickr, and
20 Telegram, to attempt to avoid detection by law enforcement. It is common for drug
21 traffickers and money launderers to install and use these apps on their phones in order to
22 make encrypted calls and send encrypted messages.

23 43. As outlined above, drug traffickers and in particular money launderers also
24 use computers to conduct their illicit activities. Many common cell phone and tablet
25 messaging applications, including but not limited to WhatsApp and Apple's iMessage
26 have counterparts on laptop and desktop computers. In addition, as outlined above, it is
27 common for individuals, including in particular money launderers, to access online
28 banking information via a computer.

SEARCH TECHNIQUES

44. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrants I am applying for will permit imaging or otherwise copying all data contained on the subject digital devices, and will specifically authorize a review of the media or information consistent with the warrants.

45. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of the subject digital devices pursuant to these warrants as follows:

a. Securing the Data

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the subject digital devices.²

ii. Law enforcement will only create an image of data physically present on or within the subject digital devices. Creating an image of the subject digital devices will not result in access to any data physically located elsewhere. However, subject digital devices that have previously connected to devices at other locations may contain data from those other locations.

//

//

² The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

1 b. **Searching the Forensic Images**

2 i. Searching the forensic images for the items described in
3 Attachment B may require a range of data analysis techniques. In some cases, it is
4 possible for agents and analysts to conduct carefully targeted searches that can locate
5 evidence without requiring a time-consuming manual search through unrelated materials
6 that may be commingled with criminal evidence. In other cases, however, such
7 techniques may not yield the evidence described in the warrant, and law enforcement
8 may need to conduct more extensive searches to locate evidence that falls within the
9 scope of the warrant. The search techniques that will be used will be only those
methodologies, techniques and protocols as may reasonably be expected to find, identify,
segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to
this Affidavit.

10 **REQUEST FOR SEALING**

11 46. It is respectfully requested that this Court issue an Order sealing, until
12 further Order of the Court, all papers submitted in support of this application, including
13 the Affidavit and search warrants. I believe that sealing these documents is necessary
14 because the warrants are relevant to an ongoing investigation into the criminal
15 organization. Premature disclosure of the contents of this Affidavit and related
16 documents may have a significant and negative impact on the continuing investigation
17 and may severely jeopardize its effectiveness.

18 **CONCLUSION**

19 47. For the reasons set forth above, I believe there is probable cause to
20 believe that evidence, fruits, and instrumentalities of violations of Title 21, United States
21 Code, Sections 841(a)(1), 846 and Title 18, United States Code, Section 1956 will be
22 found in a search of the three subject digital devices described above, which are presently

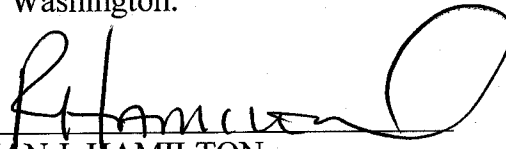
23 //

24 //

25 //

26 //

1 in the secure custody of the DEA in Tacoma, Washington.
2
3


4 RYAN J. HAMILTON,
5 Task Force Officer
6 Drug Enforcement Administration
7

8 Subscribed and sworn to before me this 10th day of October, 2019.
9


10 J. RICHARD CREATURA
11 UNITED STATES MAGISTRATE JUDGE
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A

The property to be searched is more particularly described as follows:

a. **A Red Apple iPhone in a clear protective case, marked as DEA Non-Drug Exhibit N-8.**

b. **A Black Samsung Phone in a gray and black case, marked as DEA Non-Drug Exhibit N-7.**

c. **An iPhone in a red case, marked as DEA Non-Drug Exhibit N-9.**

All of these items (collectively, the “subject digital devices”) are presently in the secure custody of the DEA in Tacoma, Washington

This warrant authorizes the forensic examination of the subject digital devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1
2 1. All records on the subject digital devices described in Attachment A that
3 relate to violations of Title 21, United States Code, Sections 841(a)(1), 841(b)(1) and 846
4 and Title 18, United States Code, Section 2, and involve Doriam German MORENO-
5 Rocha and Adrian Alberto SANCHEZ-Esparza since October 2018, including:

6 a. Evidence of the trafficking, importation, exportation, and
7 manufacture of controlled substances, including methamphetamine and heroin;

8 b. lists of customers and related identifying information;

9 c. types, amounts, and prices of drugs trafficked as well as dates,
10 places, and amounts of specific transactions;

11 d. any information related to sources of drugs (including names,
12 addresses, phone numbers, or any other identifying information);

13 e. any information recording Doriam German MORENO-Rocha and
14 Adrian Alberto SANCHEZ-Esparza's schedule or travel from October 2018 to the
15 present;

16 f. all bank records, checks, credit card bills, account information, and
17 other financial records, including all records of the transfer, deposit, wiring or other
18 transmission of funds between accounts, and records of access of financial or banking
19 sites on the internet or via applications;

20 g. all records of applications used for communication purposes and/or
21 to access financial and banking sites;

22 g. all records of communications (including but not limited to text
23 messages, internet-based messaging applications (including but not limited to WhatsApp,
24 Silent Signal, Wikr, iMessage, Skype, or similar applications and services) regarding the
25 trafficking, importation, exportation and manufacture of controlled substances and/or the
26 movement or other transfer of funds

27 h. photographs or other images (including but not limited to screen
28 captures) of controlled substances and/or of records of the deposit or transfer of funds.

1 2. Evidence of user attribution showing who used or owned the subject digital
2 devices at the time the things described in this warrant were created, edited, or deleted,
3 such as logs, phonebooks, saved usernames and passwords, documents, and browsing
4 history;

5 3. Records evidencing the use of the Internet Protocol addresses used to
6 communicate with various messaging or banking apps, including:

- 7 a. records of Internet Protocol addresses used;
- 8 b. records of Internet activity, including firewall logs, caches, browser
9 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
10 entered into any Internet search engine, and records of user-typed web addresses.

11 4. As to the wireless telephones and tablets, this warrant also authorizes the
12 following information to be searched for and seized:

- 13 i. Assigned number and identifying telephone serial number (ESN,
14 MIN, IMSI, or IMEI);
- 15 ii. Stored list of recent received, sent, or missed calls;
- 16 iii. Stored contact information;
- 17 iv. Photographs as noted above, or photographs that may show the user
18 of the phone and/or co-conspirators, including any embedded GPS
19 data associated with these photographs; and
- 20 v. Stored text messages and emails as noted above including Apple
iMessages, Silent Circle, Wikr, Facebook messenger, Blackberry
Messenger messages or other similar messaging services where the
data is stored on the telephone.

21 As used above, the terms "records" and "information" include all of the foregoing
22 items of evidence in whatever form and by whatever means they may have been created
23 or stored, including any form of computer or electronic storage (such as flash memory or
24 other media that can store data) and any photographic form.

25

26

27

28